Ubiquitous Access Control and Policy Management in Personal Networks

Dimitris M. Kyriazanos, George I. Stassinopoulos
Institute of Communication and Computer Systems,
National Technical University of Athens (ICCS-NTUA),
Athens, Greece,
dkyri@telecom.ntua.gr, stassin@cs.ntua.gr

Neeli R. Prasad
Center for TeleInFrastruktur,
Aalborg University (CTIF-AAU).
Aalborg, Denmark,
np@kom.aau.dk

***Abstract*— In this paper the authors present the challenges for enabling Security Policies Management and subsequent Ubiquitous Access Control on the Personal Network (PN) environment. A solution based on Security Profiles is proposed, supporting both partially distributed architectures –having in this case distributed master devices acting as access points- and also pure peer-to-peer interactions inside the PN. Taking benefit from the modularity and scalability of the design, this solution can be extended into supporting coalitions of different security domains, deriving from the creation of PNs federations.**

Keywords- ubiquitous access control; policy management; personal networks, secure service discovery; security profiles

I. INTRODUCTION

A personal network (PN) is the set of all networking-capable devices that someone uses for personal purposes including telecommunications, financial transactions, information, entertainment, etc. They are characterized by reduced dimensions and weight (which makes them wearable) and varying computing power and input/output capabilities. See figure 1 for a representation of the physical layout of a PN. The PN includes a dynamic collection of personal nodes and devices around a user known as the Private Personal Area Network or P-PAN, and remote personal nodes and devices in different clusters (e.g. home cluster, office cluster, car cluster) that are connected to each other through the infrastructure networks, such as cellular networks and Internet or in an ad hoc hop-by hop manner. Such a network has a very dynamic structure and usually lacks a central entity to broker the trust between its components. Despite this "ad-hoc" environment, the security requirements for a PN are very strict, because the resources it interconnects contain a significant amount of personal information (like contact lists, bank accounts, passwords or various preferences).

Security requirements in the mobile ad-hoc nature of the PN environment in a high-level point of view are no different than security requirements for any other communications system, i.e:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Access-control
- Availability

However, from a security point of view, the PN environment can be considered an extreme case. The PN, as an overlay network of mobile, wireless ad-hoc networks poses the following challenges to security experts: lack of infrastructure and a dynamic, ephemeral status of each device inside the PN. Moreover, since this is a Personal network, any required human interaction, administration and management is dependant on average every-day users, lacking security "threat awareness" and specific technical knowledge.

In this paper, the authors describe the security mechanisms and administration tools for enabling security policy management and access control on the overlay challenging environment of the PN and the PNs federation, i.e. PNs coalition.

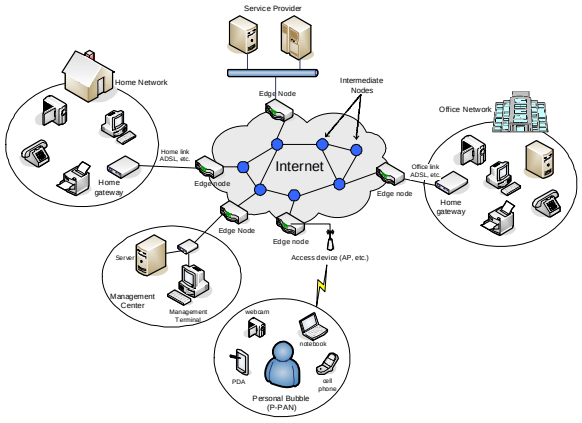

Figure 1. The physical layout of a Personal Network

II. SECURING SERVICE DISCOVERY AND PROVISIONING

In [1] an imprinting protocol based on the Diffie-Helmann exchange is described. The imprinting procedure builds a security infrastructure on top of which solutions for securing the Service and Application Level activities can be deployed.

Considering the Network Level communication secure by subsequent cryptographic material from the imprinting procedure, in order for the MAGNET service discovery and provisioning platform [2] to be considered secure on Service Level it must mainly ensure the following:

- During service discovery, a service should only be announced to authorized users according to service visibility policies.
- During service provisioning, a service should be accessed only by authorized users according to service access policies.
- Policies should be issued, stored and applied in a secure way by the administrator.

In order to provide this security, the Security Profiles, the Profile-Driven Access Control and Profile – Policy Management components were implemented.

The Profiles provide structured information about all PN elements along with related *security policies*. This structured information is kept separately from the Management and AAA application logic. The application logic is provided with the implementation of the Profile Management and Profile-Driven Access Control components. In this way, all implemented components are generic, promote extensibility and scalability while on the other hand are also able to provide security solutions to service discovery and provisioning platforms with minimum integration effort.

III. SECURITY PROFILES

All elements of the PN/P-PAN are to be described by an XML-based profile description. These profiles description will provide the necessary information needed to not only communicate between the different parties (devices and users) that constitute the PNs but also to help in the identification and authentication of the parties in communication by providing information such as name, user ID, address, job information, hobbies, favorites, password, public key, etc. The profiles will also allow the tailoring preference of services delivered to each party based on their preferred choices of preferred levels for service access (LOW, MEDIUM, HIGH), allowed levels (NEVER ,ALWAYS, CHECK) and the required security levels (Distrust, Unknown, Trust, Complete Trust). They will also allow device type dependent description (Computation power, battery life, memory size, etc…) that will help in making decisions into the quality of the service to be delivered (bandwidth limit, capacity to handle video, sound and GUI, etc).

Keys resulting from subsequent cryptographic mechanisms based on the imprinting procedure, when present in any profile description, must be handled with care, never to divulge any private key during any exchange of profiles to any outside party.

A. User Profile

The User description will hold all necessary information about the user (owner of the P-PAN or any node an outsider user uses to access the P-PAN for a service).

The User module is subdivided into two main parts:

- User information: this part assemble all the information related to the person/user, such as name, user ID, address, job information, hobbies, favorites, etc.
- Access information: this part assemble all the information related to the access policy and security, such as preferred levels for service access (LOW, MEDIUM, HIGH), allowed levels (NEVER ,ALWAYS, CHECK), the user private keys, public keys, and other's public keys, the security service levels (LOW, MEDIUM, HIGH), etc.

B. Node Profile

The Node description will hold all necessary information about the node (device) that is part of the user/owner's P-PAN or any device, node, which an outside user can use to access a P-PAN for a service.

The node module is subdivided into four main parts:

- Device Information: this part assemble all the information related to the device, such as device type, manufacturer name, battery life, computing power, friendly device name, model name, model number etc.
- Optional Information: this part assemble all the information related to the device, such as manufacturer URL, model URL, serial number, unique device ID number, icon service list, etc…
- Service List: this part assemble all the information related to the person/user, such as name, user ID, address, job information, hobbies, favorites, etc…
- Context: this part assemble all the information related to the access policy and security, such as preferred levels for service access (LOW, MEDIUM, HIGH), allowed levels (NEVER ,ALWAYS, CHECK), the user private keys, public keys, and other's public keys, the security service levels (LOW, MEDIUM, HIGH), etc.

In addition to the four main parts, information such as the unique node ID number and the presentation URL of the node that holds this node are provided.

C. SMN Profile

The MAGNET service discovery is centralized at the P-PAN/cluster level and fully decentralized at the PN level [6]. In this regard, a *Service Management Node* (SMN) is introduced that discovers and manages the services in the P-PAN/cluster level and interacts with the other SMNs at the PN level. At the P-PAN/cluster level, each SMN is responsible for the global secure service management and centralizes the information/description of available services. It is also responsible for remote service discovery and advertisement. In the PN level, the entire cluster SMNs communicate with each other to discover services that are already registered in the PN.

The SMN module is subdivided into five main parts:

- Service List: this part assemble all the information related to the person/user, such as name, user ID, address, job information, hobbies, favorites, etc…
- Group Profile: this part assembles all the information related to the group profiles, such as group name, member list, membership profiles etc.

- Local Policy: this part assembles all the policy information related to the service and security etc…
- Service Trust Level List: this part assembles the trust information related to the services provide by Nodes that are accessed by Users through this SMN. The values taken by the service trust levels are Distrust, Unknown, Trust and Complete Trust.
- Reputation List: this part assembles the trust information related to the reputation of User and Node that access the services through this SMN. The values taken by the reputation level are Distrust, Unknown, Trust, Complete Trust.

In addition to the five main parts, information such as the node name, a unique node ID number, and the URL of the node that holds this SMN are provided.

D. Service Application Profile

The Service Application module is subdivided into four main parts:

- Service Description: this part assembles all the information related to the service description, such as State Table, Action List, Control and Event URL etc…
- Group Profile: this part assembles all the information related to the group profiles, such as group name, member list, membership profiles etc…
- Local Policy: this part assembles all the policy information related to the current service and security, such as service ID, service name, security level, etc…
- Service Trust Level: this part assembles the trust information related to the service provide by a Node that is accessed by Users through the SMN. The values taken by the service trust levels are Distrust, Unknown, Trust, Complete Trust. It is the SMN that manages all the trust values.
- Reputation: this part assembles the trust information related to the reputation the User-owner and the Node that provide access to this services through the SMN. The values taken by the reputation level are Distrust, Unknown, Trust and Complete Trust.

In addition to the four main parts, information such as the service name, service type, service version number, a unique service ID number, and the manufacture/developer URL are provided.

IV. PROFILE SYNTAX

In order to organize data in the profile, the Extensible Markup Language (XML) was used [3]. XML is an independent platform which has rapidly become a major technology, offering solutions anywhere data is manipulated and exchanged between applications or tiers. XML's structure offers a far more efficient and flexible representation of data and metadata in the profile, in comparison with the flat text approach.

In addition to the benefits from the use of XML itself, XML related technologies also offer a number of advantages. XML can be easily transformed with use of XSL style language. In this way, profiles can be easily transformed in order to promote interconnectivity and compatibility with other profile mechanisms. XML encryption mechanisms and XML digital signing is used to secure the integrity and privacy of the profiles.

V. PROFILE AND POLICY MANAGEMENT

Policy Management throughout the PN is achieved by properly propagating profile information updates by the PN administrator. For this purpose, a tool is provided for the policy administrator through which policies can be issued regarding entities placed anywhere inside the PN, providing policy management for the overlay network through a tree-like structure Graphical User Interface (GUI). The GUI, as shown in figure 2, guides the user through the available security preferences.

Once policies are personalized according to user interaction, propagation of policy updates throughout the PN is achieved by utilizing the SMN entities inside the PN, properly notifying responsible SMNs for any changes in their local policy settings. Device specific policies are subsequently delivered to the corresponding devices from the local SMN.

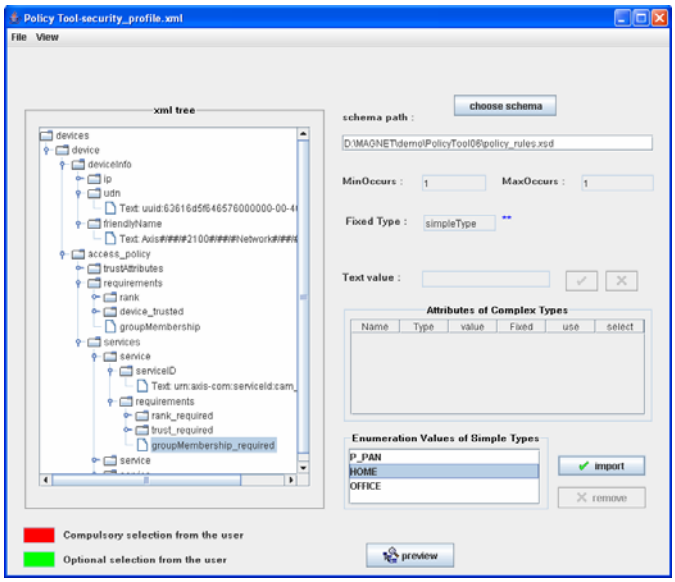

Figure 2. Policy Management GUI.

VI. UBIQUITOUS ACCESS CONTROL

Access control throughout the PN is a challenging task. Besides the lack of a centralized authority due to connectivity restrictions, connectivity is again not guaranteed to every cluster inside the PN. Therefore, certain clusters might be out of reach of the owner-administrator. With respect to these problems, the authors present here a solution for a distributed and decentralized access control system.

In each cluster, a certain Personal device is elected to act as a master device (SMN), responsible for service management and advertising. The election procedure involves a sequence of tests from which the strongest device –from a computational and networking point of view- becomes the master device. Based on the Security Profiles, access control modules and profile repositories were designed and developed to function in a distributed way throughout the overlay access control system which is formed by the interconnected set of master devices. In this way, each master device acts independently as an access policy officer for all the devices and access requests under her jurisdiction. Moreover, devices which are capable of holding profile repositories and access control modules subsequently perform access control in a decentralized way. In figure 3, the flow of a service request access control procedure is presented, depicting both the SMN based (master device) and pure peer-to-peer access control mechanisms. For devices incapable of holding such modules and repositories, such as sensors, proxies are needed.

On the other side, the user performs policy management over the entire PN network using a proper administration tool. Even in case of a cluster losing connectivity to the rest of the PN, the corresponding master device is expected to block any unauthorized access requests. However, in situations of an isolated cluster, access rights and certificate revocations issued by the PN administrator will fail to reach the master device. In order to minimize the impact of such unfortunate situations, grant of privileges and access rights below a default, high level of security should at all times be ephemeral and stamped with an expiration time. Such timestamps would reduce the risk and the extent of damage caused by exploiting lack of connectivity to the PN administration, since any expired granted rights will be revoked even by isolated nodes, equipped with the proper modules. As a future work, time-stamping techniques and modules will be developed for enhancing the PN Access Control system.

In order to test Access Control and Policy Management, related components were integrated to a scalable UPnP – INS/Twine wide-area service discovery platform [4], and were demonstrated recently as part of a Personal Network Prototype Demonstrator to the European Commission of Information Society Technologies.

Finally, any communication between modules and the policy management administration tool remains secure since it is based on the underlying security infrastructure such as mechanisms described in [1],[2] and also typical VPN security mechanisms.

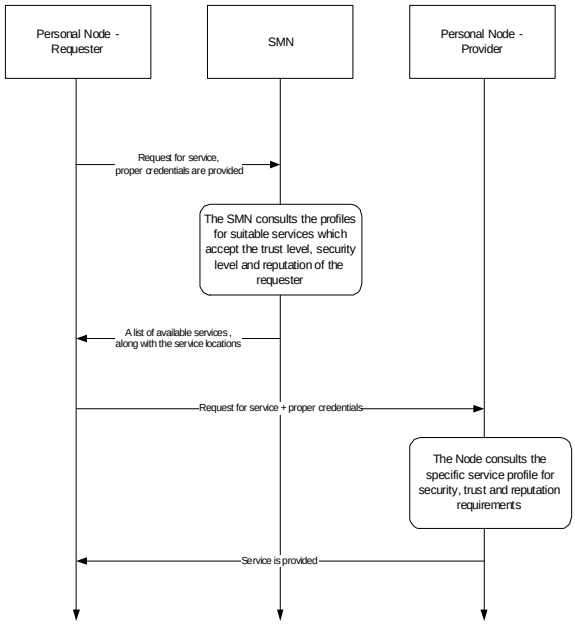

Figure 3. A successful handling of an authorized service request using Profiles.

VII. CONCLUSIONS

Distributed architectures and peer-to-peer solutions, being the most favorable choices for Personal Networks, pose considerable challenges for access control and policy management on the overlay network of interconnected clusters. Ubiquitous access control is achieved by proper propagation of Security Profiles to delegated master devices acting as "access points". Policies related to specific devices are also stored in the device itself -or a proxy if the device is e.g. a sensor- in order to enable access control in a pure peer-to-peer way. Situations where certain parts of the PN would be unreachable at the time of issuing a new policy are dealt by proper querying at the time of reconnection. However, time stamping mechanisms are also required so as to minimize the risk of someone abusing outdated rights inside an isolated cluster.

ACKNOWLEDGMENT

This work has been performed in the framework of MAGNET and of its continuation MAGNET BEYOND, IST Projects partly funded by the European Union. The authors would like to acknowledge the contribution of their colleagues from the consortium's Work Package 4: "Security and Privacy".

REFERENCES

[1] Personal Network Security Architecture, C. Politis, K. Nyberg, S. Mirzadeh, K. Masmoudi, H. Afifi, J. Floroiu, N. R. Prasad, , International Wireless Summit 2005, Wireless Personal Multimedia Communications'05, September 18-22, Aalborg, Denmark.

[2] MAGNET Secure Service Discovery Architecture. Shahab Mirzadeh, Khaled Masmoudi, Yacine Rebahi, Neeli R. Prasad, Christos Politis and Hossam Afifi, International Wireless Summit 2005, Wireless Personal Multimedia Communications'05, September 18-22, Aalborg, Denmark.

[3] http://www.w3.org/XML/, Extensible Markup Language (XML) World Wide Web Consortium (W3C) site.

[4] Implementation of UPnP and INS/Twine interworking for scalable wide-area service discovery, W. Louati, M. Girod-Genet, D. Zeghlache, WPMC 2005, Denmark, 2005.

[5] http://www.ist-magnet.org, IST-507102/MAGNET project site.

ABOUT MAGNET BEYOND:

MAGNET Beyond is a continuation of the MAGNET project (www.ist-magnet.org). MAGNET Beyond is a worldwide R&D project within Mobile and Wireless Systems and Platforms Beyond 3G. MAGNET Beyond will introduce new technologies, systems, and applications that are at the same time user-centric and secure. MAGNET Beyond will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. MAGNET Beyond has 32 partners from 15 countries, among these highly influential Industrial Partners, Universities, Research Centers, and SMEs.